IMPROVING THE EFFICIENCY OF SIP AUTHENTICATION BASED ON THE PRE-CALCULATED LOOK-UP TABLE

By
AWS NASER JABER

UNIVERSITI SAINS MALAYSIA

2013

IMPROVING THE EFFICIENCY OF SIP AUTHENTICATION BASED ON THE PRE-CALCULATED LOOK-UP TABLE

By

AWS NASER JABER

Thesis submitted in fulfillment of the requirements for the degree of Master of Applied Science

May 2013

ACKNOWLEDGMENT

I would like to take this opportunity to convey my sincere thanks and deepest gratitude to Prof. Dr. Sureswaran Ramadass, and Mr. Selvakumar Manickam for all their help and valuable guidance provided to me during the preparation of this thesis. I consider myself privileged to have had the opportunity to work under his guidance.

Moreover, I would like to dedicate this thesis to the dearest ones, my father for his patience and the encouragement he provided me with during the entire period of the study, and my mother who shared the stress in my life, encouraged me in times of dismay, cheered me up in times of distress, and renewed my hope in times of despair.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

ASCII	American Standard Code for Information Interchange
CIA	Confidentiality, Integrity, Availability
DH	Diffie–Hellman
DLP	Discrete Logarithm Problem
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie- Hellman
ECDL	Elliptic Curve Discrete Logarithms
HTTP	Hyper Text Markup Language
IETF	Internet Engineering Task Force
IP	Internet Protocol
IT	Information Technology
ITU	International Telecommunication Union
PSTN	Public Switched Telephone Network
RFC	Request for Comments
RSA	Rivest, Shamir and Adleman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SCTP	Stream Control Transmission Protocol

SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SRTP	Secure Real Time Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
ToIP	Text over Internet Protocol
UA	User Agent
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol

MENAMBAH BAIK KEEFISIENAN PENGESAHSAHIHAN SIP BERDASARKAN JADUAL RUJUKAN PRA-HITUNGAN

ABSTRAK

Telefon IP telah mendapat manfaat yang besar daripada keupayaan yang semakin meningkat perkakasan komputer secara umum, termasuk mikropemproses yang lebih cepat, memori yang lebih besar kapasiti, dan rangkaian jalur lebar yang lebih besar. Sebuah telefon IP tunggal perkapalan pada tahun 2010 mempunyai kapasiti pengkomputeran yang jauh lebih daripada kebanyakan daripada PBX awal. Trend ini hanya akan terus.

Telefon IP menambah memaparkan warna dengan pelayar web besar-besaran. Ada menambah tertanam Amaran Jangan lupa untuk menyiasat bagaimana data disimpan pada sistem tempatan atau mana-mana sistem perantara. Jika, misalnya, semua fail log IM chat sesi disimpan dalam jelas, tanpa enkrip teks pada komputer tempatan di mana beberapa orang mempunyai akses kepada komputer, hakikat bahawa klien IM menyulitkan sesi antara komputer dan pelayan tidak melindungi sepenuhnya sesi-sesi.

Transkrip sesi masih boleh dibaca tempatan oleh sesiapa sahaja yang mempunyai akses kepada komputer tempatan.
Hari ini, sementara masih banyak syarikat mungkin memilih untuk membeli dari penjual tunggal demi kemudahan, realitinya adalah bahawa dalam era piawaian

protokol kendali seperti Protokol Permulaan Sesi (SIP), syarikat-syarikat tidak lagi diperlukan untuk membeli dari yang sama penjual.

Protokol isyarat ‘Session Initiation Protocol’ (SIP), kebelakangan ini telah menjadi keutamaan dalam aplikasi-aplikasi Internet. Perkembangan besar dalam perkhidmatan SIP, kebimbangan dalam keselamatan SIP semakin meningkat.

Oleh itu, pengesahsahian SIP yang terkenal telah dikaji. Dari kajian ini, suatu perbaikan pada kriptografi skema terbaru yang dikenali sebagai skema Yoon, yang dicadangkan adalah efisien pada keselamatan pengesahsahian SIP tetapi tidak pada masa dan pretasi pemprosesan.

Oleh itu, ia membawa kita untuk memperkenal cara peningkatan skema pengesahsahian SIP berdasarkan ‘Elliptic Curve Cryptography’ (EEC) dengan jadual rujukan dan pendaraban scalar.

Malah, hipotesis yang dicadangkan adalah untuk mengatasi dan bandingan kos masalah kedua-dua skema pengesahsahian yang dikaji terdahulu.

Walau bagaimana pun, persoalan disini adalah bagaimana penyelidikan ini boleh meningkatkan efisien tanpa kemerosotan pada tahap keselamatan.

Hasilnya, ECC adalah paling banyak mengguna masa operasi berbanding dengan operasi-operasi lain seperti ‘EXCLUSIVE OR’ dan fungsi ‘hash’. Pengurangan bilangan ECC dengan pencegahan kemerosotan keselamatan adalah sangat penting dan ia akan meningkatkan kelajuan komunikasi dengan kependaman yang kurang.

IMPROVING THE EFFICIENCY OF SIP AUTHENTICATION BASED ON THE PRE-CALCULATED LOOK-UP TABLE

ABSTRACT

IP phones have benefited greatly from the ever-increasing capabilities of computer hardware in general, including faster microprocessors, larger memory capacity, and greater network bandwidth. A single IP phone shipping in 2010 has far more computing capacity than most of the early PBXs. This trend will only continue. IP phones are adding color displays with full-blown Web browsers. Some are adding embedded Warning Do not forget to investigate how data is stored on a local system or any intermediary system. If, for instance, all log files of IM chat sessions are stored in clear, unencrypted text on a local computer where multiple people have access to the computer, the fact that the IM client encrypts sessions between the computers and the server does not fully protect those sessions. The session transcripts could still be read locally by anyone with access to the local computer. Today, while many companies might still choose to buy from a single vendor for the sake of convenience, the reality is that in the era of interoperable protocol standards like Session Initiation Protocol (SIP), the companies are no longer required to buy from the same vendor. The session initiation protocol (SIP) has recently become the main signaling protocol for Internet applications. The wide range of SIP services raises many concerns on SIP security. Thus, the most popular SIP authentication schemes were studied in this paper. The previous cryptographic scheme known as Yoon's scheme proposes SIP authentication that brings efficiency in security but is costly in terms of time. Our proposed scheme is an improvement of Yoon's scheme,

as it enhances SIP authentication based on elliptic curve cryptography (ECC) with look-up tables and scalar multiplication. A hypothesis was proposed to overcome and compare the cost problems with the two authentication schemes. However, the research question is how to make the proposed scheme more efficient without decreasing the level of security. Thus, ECC was developed to become the most time-consuming operation compared with other operations such as “EXCLUSIVE OR” and “hash functions.” Decreasing the number of ECC while preventing the degrading of security is very important, as it increases the speed of communication and reduces latency.

CHAPTER ONE

INTRODUCTION

The telecommunications, television, and information technology (IT) network industries are all transformed by the Internet. The transformation is driven by the need for growth based on new services, more complete global coverage, and consolidation.

With new communications technologies, there is always the temptation to mimic the old. E-mail inherited aspects of the interoffice memo and fax; web pages attempted to look like newsprint and brochures. However, in VoIP, there is the particular temptation to recreate old technology features, as interoperability with the old PSTN will remain important for at least another decade. Fax-to-email gateways were never quite as important as VoIP-to-PSTN gate-ways. This emphasis on interoperability with 100-year-old technology has provided a financial motivation—provides the same service more cheaply. However, this may also hold back the promise offered by Internet-based multimedia communications, such as the integration of presence, the ability not just to communicate by voice and maybe video but also to share any application, or the ability to customize the user experience and integrate interactive communications with existing Internet tools and applications. Just as most microprocessors are embedded in household appliances and cars, not desktop PCs and laptops, we might find that Internet-based voice and multimedia communications will be integrated into games, appliances, and cameras, or be hidden behind a link on a web page, rather than dialed by name or number. As for many of the most innovative applications, users will likely not even consider them phone services at all, but extensions that make some other application more productive or more fun.

The Internet was originally not reliable enough and lacked the capacity to carry voice and video traffic. IP was built around the expectation of unreliable connectivity with the ability to recover. Generally there was little or low impact to data applications at the time, in the event of momentary/temporary service disruption.

Although the Internet has quickly established itself as the preeminent network for data, commercial transactions, and audio-video distribution, the use of voice over the Internet has been slower to develop. This has less to do with the capability of the Internet to carry voice with equal or higher quality than the telephone network but rather with the complex nature of signaling in voice services.

There are in fact, three come on voice servers over internet, which is based on several signaling and control design system. Some examples include the following:

- Using *signaling* conception form the telephone industry, for example, Media Gateway Control Protocol (MGCP), Gateway Control Protocol (H248) and H323.
- Using the control concepts from the large telephone enterprises, for example, soft switch and central control.
- Using the internet - centric protocol- session initiation protocol (SIP).

Meanwhile, circuit switch dedicated communication path between two stations. Further, a three main phases for circuit switch which is: establishment, transfer and disconnect that must have switching capacity and channel capacity to establish connection. In addition it must have intelligence to work out routing figure 1.1, shows the circuit switch.

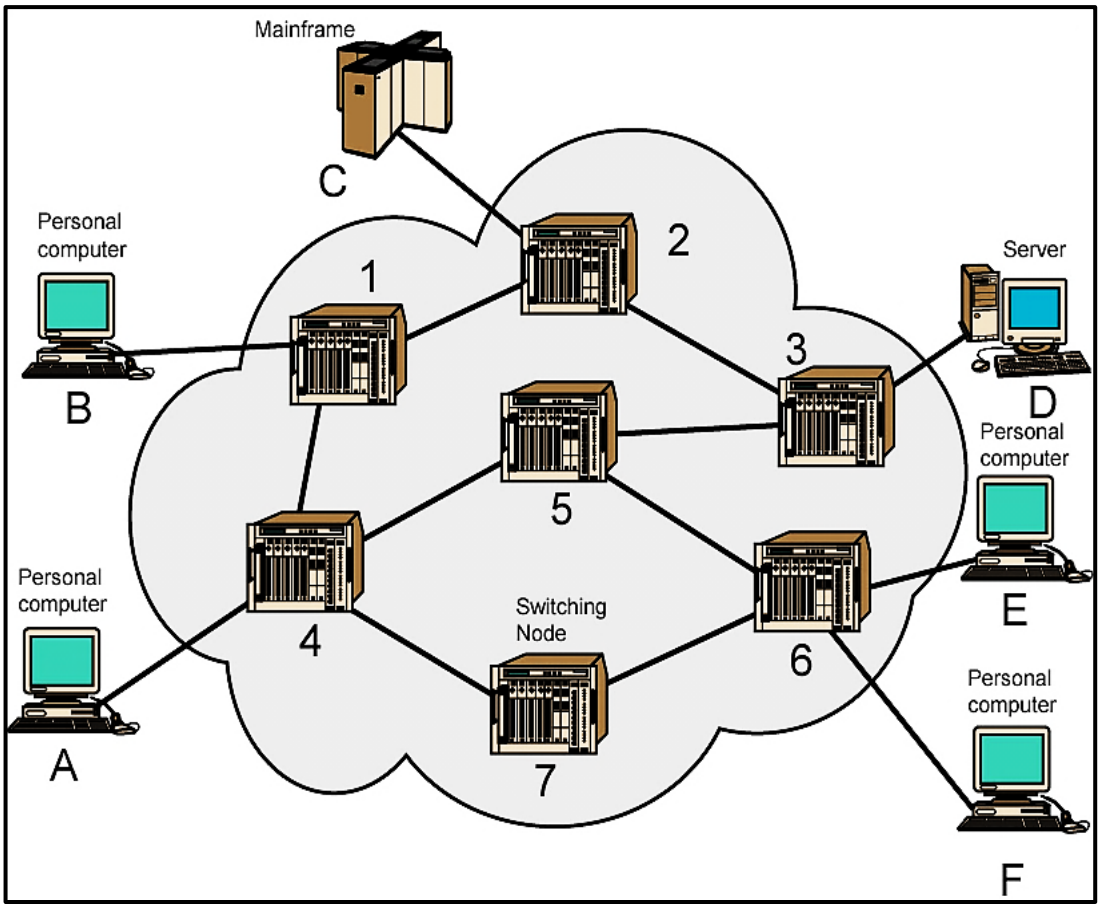

Figure 1.1: Circuit-switching system.

By contrast, packet-switching protocols are designed for voice resources dedicated to a particular call. In the packet-switching system, much more time is needed, and a larger amount of data is idle; however, the data rate is fixed, and both ends must operate at the same rate. The details of the basic system operation are as follows:

- Data transmitted in small packets:
- Control information:
- Packets are received, stored briefly (buffered), and passed on to the next node
    - Packets are stored and forwarded.

Figure 1.2 illustrates the use of packets.

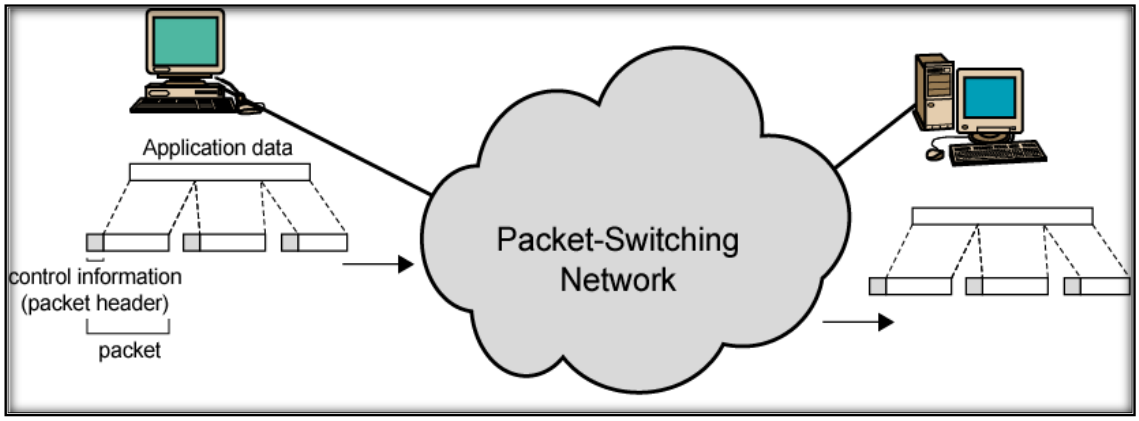

Figure 1.2: Packet –switching network

Nowadays, the Internet can serve three functions for telecommunication and VoIP; through the Internet, we can transmit voice packets, video packets, and both voice and video packets (Figure 1.3).

While, the information technology (IT) network industries, telecommunications, televisions are all transformed by the internet. The transformation led to growth based on new application servers, more feasible and easy to deal with global coverage and conduction.

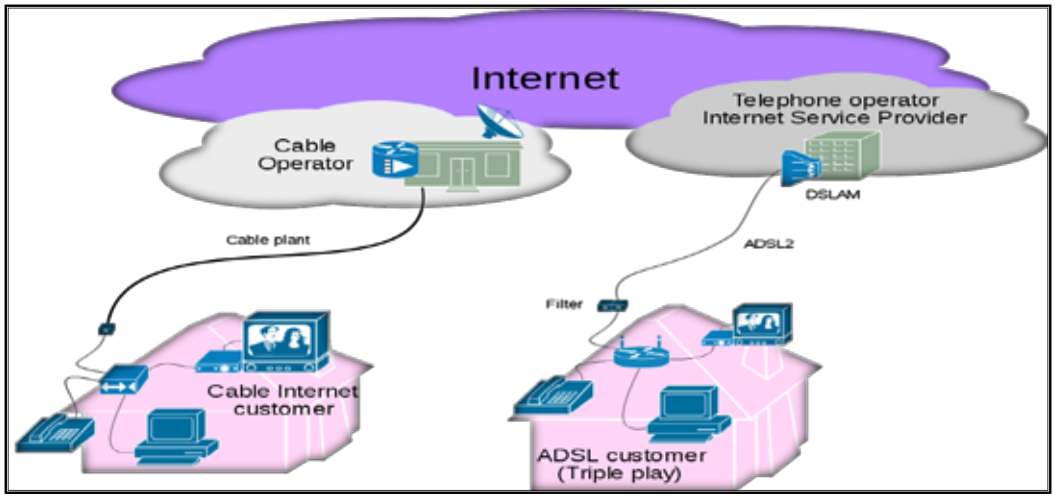

Figure 1.3: The voice packet transmission

SIP is not just another protocol. SIP redefines communications, and is impacting the telecom industry to a similar or greater degree than other industries. This has been recognized by all telecom service providers and their vendors for wired and wireless services as well as in (Figure 1.4) shown all vendors that supported SIP. Many networks and service provider see it as a cost-cutting proficiency. Furthermore, VoIP infrastructure is an economic foundation on which new revenue generating services are invented by the providers.

Latently, envisioned SIP services are termed as converged services. Several proficient features, and functions present in existing services have been effectively incorporated into these recent SIP services. Certain features have been adapted from conventional voice-based telephony services and then combined with features from data network services. For example, in using a click-to-dial service, users can control telephone calls, SMS, and callbacks via a web browser running on their personal computer systems. Converged services offer users new media integration such as multimedia conference. This multimedia service allows users to communicate with each other via calls with an effective exchange of audio and video information. Several new versions of video phones are examples of such transmission.

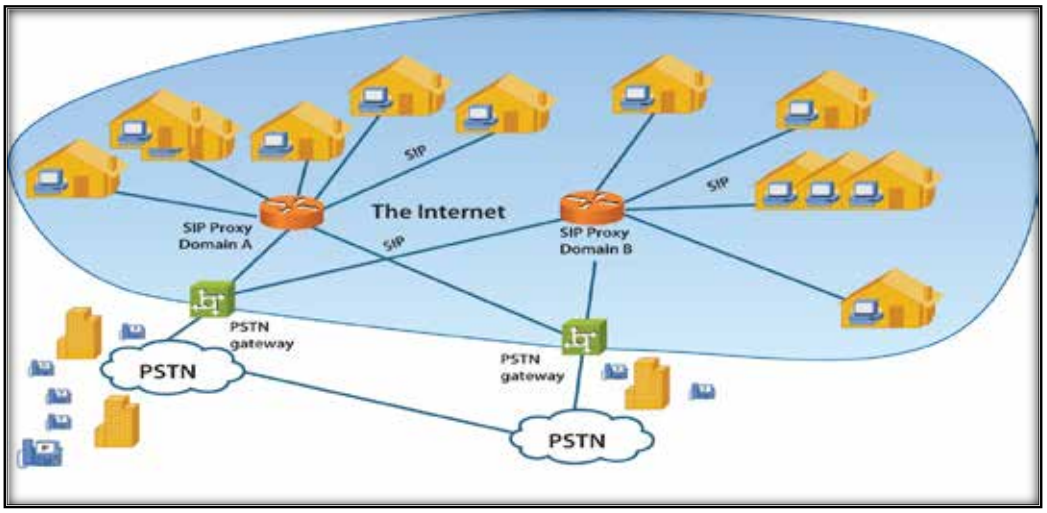

Figure 1.4: SIP distribution and usage

1.1 Background

SIP-based VoIP services have gained popularity compared with other supplementary protocols such as the MGCP (e.g., Media Gateway Initiation Protocol or H.323) despite their susceptibility to various attacks akin to those active ones on the Internet. As a formal way to describe VoIP vulnerabilities has not been established, the development of tools required in identifying vulnerabilities or testing the security level of offered services is obstructed. These tools are independent from specific implementation in both cases.

The SIP (Garcia-Martin, Belinchon, Pallares-Lopez, Canales-Valenzuela, & Tammi, 2006) is implemented basically as a signaling protocol to deal with multimedia sessions on the Internet and 3G realms. Researchers have proposed various security mechanisms for SIP-based infrastructure, yet certain vulnerabilities have an impact on this architecture. These vulnerabilities affect the architecture in a number of ways, including attempting to deplete available resources, creating fake

reactions in response to malicious requests, and trying to discover possible vulnerabilities in the application.

The SIP is the preferred signaling protocol in current and future IP telephony services, thereby becoming a competitor for traditional telephony services. However, the open architecture of the SIP has resulted in the vulnerability of provided services to different types of security threats on the Internet, such as spoofing, hijacking, and message tampering(Nucci, Ranjan, & Zhang, 2012).

These attacks could result from misconfiguration on the server or from using the default server security policy for the SIP server. A Denial of Service (DoS) attack can occur with many VoIP attack tools such as the SIP Crack (McGann & Sicker, 2005).

1.2 VoIP Encryption

Signaling and media are the two forms of VoIP encryption. Control channels for the SIP or H.323 communications are protected by signaling encryption and the Real-time Transport Protocol (RTP) (Venna, Stratton, Hedayat, Jones, & Kaplan, 2012) streams used in voice, video, or fax that are protected by media encryption. The purpose of the key in signaling encryption is to prevent leakage of sensitive information.

Modern SIP specifications offer several approaches in securing signaling. One such method is Transport Layer Security (TLS) (Dierks, 2008) ,which an identical technique utilized in securing web connections and in encrypting SIP signaling from one device to another. However, TLS is unable to ensure top security

level for end-to-end encryption. Nonetheless, it introduces a significant provision and performance overhead to an SP connection.

The rationality behind this advantage is that TLS can flow only over the transmission control protocol (TCP), and a certificate infrastructure is a prerequisite to enabling this flow between communicating parties. As such, carrier-grade SIP deployments have yet to implement secure TLS signaling. To date, researchers have been unaware of carriers offering enterprises with secure signaling or media on SIP trunks.

However, In encrypting the body and sensitive headers of an SIP message using Secure/Multipurpose Internet Mail Extensions (S/MIME)(Schaad, 2012), and certificate-based cryptography, a standard is available for end-to-end SIP signaling encryption. However, despite the existence of an SIP standard for S/MIME key exchange, its implementation remains complex. Furthermore, this part of the standard is hardly supported by SIP products.

Although not commonly supported, the TLS is also an option for H.323 in signaling encryption. Parts of the H.323 standard support effective encryption of sensitive signaling elements, thus offering efficient signaling encryption without using Public Key Interface.

Even though numerous vendors encrypt signaling in their devices, securing signaling among H.323 solutions from distinct vendors is extremely difficult. Therefore, an extremely effective key exchange mechanism has been proposed for

the user agent (UA) server in an SIP environment. Figure 1.5 shows a good example of the SIP with public key.

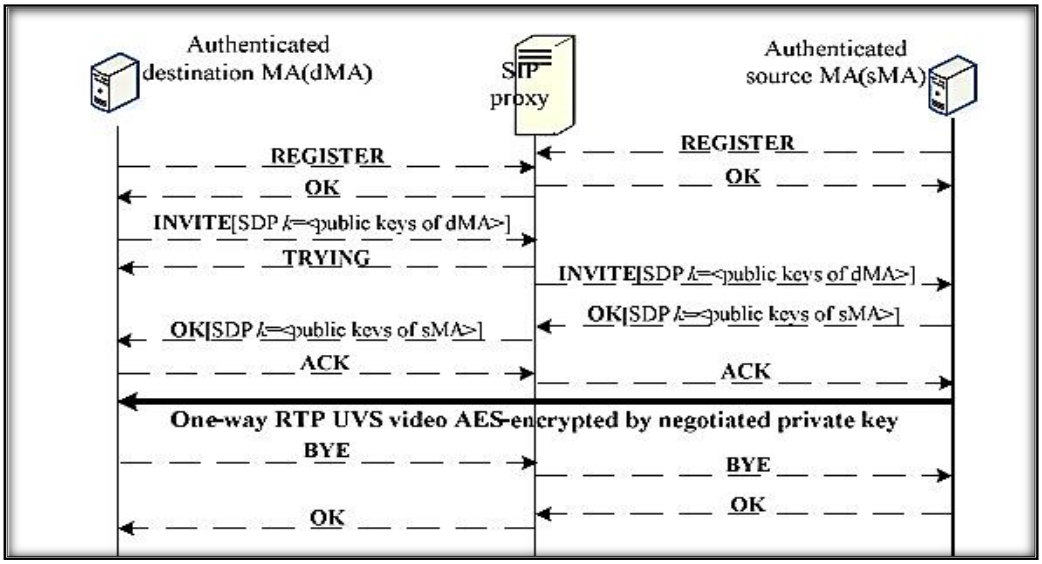

Figure 1.5: Key exchange with public key through SIP proxy server

1.3 Problem Statement

SIP deployment faces many issues, such as detecting, monitoring, and mitigating security threats. It bears the risks of many new ways to attack SIP servers and their extensions in enterprises or campuses.

Although the SIP is grounded from HTTP digest authentication, the protocol is still vulnerable to brute force attacks, and weak passwords tend to be identified easily using dictionaries. A comparison of results is still possible through the applied signature algorithm. The HTTP digest authentication is a good example; it is used in several applications because of its extremely convenient implementation and exceptional performance.

However, attackers can effortlessly pick out crucial information about the authenticated SIP authority holder. This information can be used to acquire details regarding “Log on” and enable the attacker to make calls.

Researchers have proposed various schemes for SIP signaling to overcome the weakness of VoIP digest authentication. They have tried to address more threats by using more cryptography techniques and by increasing the number of authentication steps. The consequence of these efforts is more security but less efficiency. Thus, a large number of studies have intensively covered the issue on attacks but have failed to consider the costs entailed and the inadequate storing for cost. A type of balance or enhancement of the encryption world is thus needed. Based on the above, a different methodology is adopted in this work, which deserves a customized research method.

1.4 Thesis Objective

The objectives of this study are as follows:

- To devise this problem by presenting a proposed method to secure, and develop the SIP register user server and their clients by considering the problem and finding out results.
- To review and assess current SIP security mechanisms, surveys on the hurdles faced by the present SIP security, and the methods used by related studies to conquer such hurdles. We hope to initiate a study on SIP to prevent security leak.
- To examine the efficiency of the proposed scheme compared with other relevant schemes on SIP confidentiality in terms of cost performance.

1.5 Research Contribution

The primary contribution of this research is the proposal of an improved authentication scheme for the SIP that offers significantly more efficient services. The goals of the proposed scheme are as follows:

- **Efficiency:** To increase the efficiency of the security mechanism by identifying costly operations, reducing the number of operations by separating them into two groups, namely, off-line and online operations, and by then by shifting the operations from the online to the off-line group without degrading the level of security.
- Security: To develop an authentication scheme that increases the level of security for SIP clients and their servers.
- Designing inherently robust and resilient crypto-SIP server and clients

1.6 Thesis Organization

This research consists of the following six chapters:

1. **Chapter 1**: presents a general overview of this thesis.

2. **Chapter 2**: briefly introduces the basic underlying concepts, including the basics of the SIP, SIP security mechanisms, as well as the nature of different kinds of attacks and how they degrade the performance of an SIP system. This chapter also reviews the proposed solutions and strategies for solving the security issues.

3. **Chapter 3**: discusses the proposed authentication scheme.

4. **Chapter 4**: presents a comparative analysis of deploying the SIP-based VoIP system using our model test scenario.

5. **Chapter 5**: presents the results and references.

6. **Chapter 6:** is the conclusion.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The SIP dominates protocols that establish, modify, and end multimedia sessions such as conferences. The SIP is designed for signaling multicast call flow. The Request for Comments (RFC) 3261 (Rosenberg et al., 2002) defined by the Internet Engineering Task Force is designed specifically for the control of real-time multimedia communications. The intention is not to limit the requirement for supporting voice calls, but to create a specific control protocol capable of supporting all forms of communication. SIP attacks and SIP-related protocol attacks are discussed in this chapter. As our focus is security protocol, the number of potential attacks on SIP and SIP-related protocols is also discussed, with the importance of high security levels considered.

2.2 SIP

Signaling in telephone systems is the key mechanism by which telephone calls are set up and terminated. For example, signaling from a desktop business phone tells the PBX to forward the call to another phone. In the public telephone network, signaling instructs the switching systems to forward, for example, an 800 call to a specific call center where an agent will answer the call.

An example of the value of signaling is the comparison between a telephone chat between two residences, and an 800-number call to a customer-support center. Such calls are also priced differently. In the end, both phone calls sound the same, except that signaling has enabled the adding of commercial value to the 800 number calls for a possible business transaction. Signaling defines the desired service for the

user, such as point-to-point calls, multipoint conferencing, Centrex services, text, voice, and video, and others.

Thus, the signaling protocol for Internet multimedia real-time communications is the Session Initiation Protocol (SIP). SIP is one of the most famous signaling protocols used to identify signaling encapsulation. The state of connection between telephones, or VOIP terminals (IP telephone , PCs and Voice over Wireless (VoWLAN) units can be initialized by Signaling ;It is always important to understand the voice protocols against the OSI model to situate where each protocol fits(Knightson, Morita, & Towle, 2005) and figure 2.1 explain it in deeply.

The SIP actually uses HTTP headers that bring many advantages to the SIP, including URL dialing and better session routing for all packets. Several programs that we use are built on this great technology.

The RFC 3665 lists 11 fundamental session establishment flows (Johnston, Donovan, Sparks, Cunningham, & Summers, 2003). This list is not intended to be comprehensive, but it covers best practices, that is, “successful session establishment” and “session establishment through two proxies.” However, other sessions, such as “unsuccessful with no answer” and “unsuccessful and busy,” are addressed in the following chapters dedicated to call forwarding.

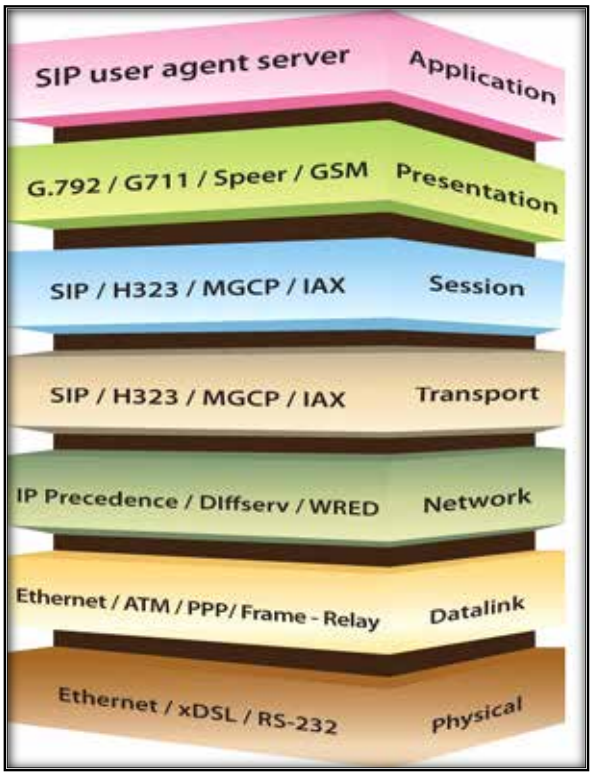

Figure 2.1: SIP location between OSI models

However, SIP messages can also be transferred via wireless networks (Schulzrinne & Wedlund, 2000). However, message transfer via such networks also suffers from security weakness and leakage on authentication procedures, for example, signaling the packages and eavesdropping in the packages and eavesdropping by the media between end to end points.

2.2.1 SIP Structure

SIP messages have two types: “request” and “response.” An SIP request can be one of the following: REGISTER, to notify the SIP domain registrar about user location; INVITE, to establish a session; BYE, to terminate a session; CANCEL, to drop any established session; OPTIONS, to ask another user or server about its capabilities; and MESSAGE, to send instant messages. SIP response is the

acknowledgment or ACK message used to confirm the receipt of a “200 OK” replies. A full SIP message consists of two parts separated by an empty line: header and body. All SIP messages, except INVITE and MESSAGE, do not need a body.

In addition, an SIP user needs an address/identifier to communicate with others, and this address is written in a Uniform Resource Identifier (URI) format (Masinter, Berners-Lee, & Fielding, 2005).

2.2.2 Session Description Protocol (SDP)

The SDP (Handley, Jacobson, & Perkins, 2006) described in RFC 4566 is used as a tool to negotiate session parameters between UAs. It is applied in the exchange of media details, transport addresses, and other media-related information between UAs. The INVITE message usually carries the SDP offer message, whereas 200 OK contains the response to the INVITE message.

2.2.3 SIP Messages

The SIP message header consists of two parts, namely, the first line and the rest of the header. The first line contains the request type, that is, the Request-URI, and the SIP version. The Request-URI should initially have the same value as the field, but it can be set to the next hop identifier as well. The first line in a response-type message includes the response code, as shown in Table 2.1.

Table 2.1: Overview of SIP response messages

Description	Status code	Example
Informational	1xx	100 Trying
Success	2xx	200 Ok
Redirection	3xx	300 Multiple choices
Client error	4xx	400 Bad request
Server error	5xx	502 Bad gateway
Global failure	6xx	603 Decline

As depicted in the table, SIP response messages have six categories, namely, informational response (1xx); success (2xx), which indicates the successful delivery of information and request; redirection (3xxx), wherein the user can find alternative service by temporarily using proxy if the address has moved permanently; client error (4xx), which indicates that the request must proceed through proxy; server error (5xx), which refers to server failures; and global failure (6xx), wherein topical request cannot respond to the server.

- Requests

    1. INVITE – to initiate a session.

    2. ACK – to indicate receipt of the corresponding messages.

    3. BYE – to terminate a session.

    4. CANCEL – to stop a previous request.

    5. REGISTER – to send registration details to a registrar.

6. OPTIONS – to query another UA or a proxy server with regard to its capabilities.

2.2.4 SIP Call Establishment

The RFC 3665 (Johnston et al., 2003), provides a detailed description of the basic call flow. For example, the calling party “2011” sends an invite request message, thereby initiating a message exchange with the destination party “2012” for establishing calls. That invite message contains all details of the call or the requested session, such as a video conference or an online gaming session(Singh & Acharya, 2005).

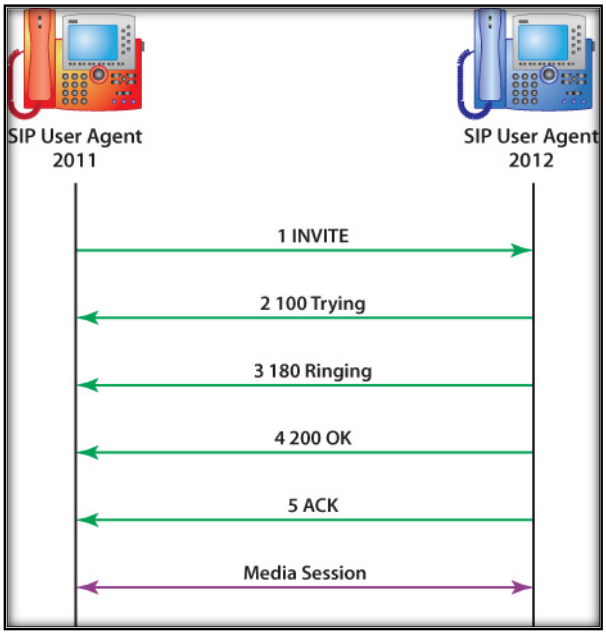

Figure 2.2: Displayed the process of exchange of two SIP messages with each other.

When the invite request is sent by “2011” to “2012,” the request would contain the type of requested session, that is, either a video conference or a simple online gaming session.

2.2.5 SIP Call with a Proxy Server

Proxy servers are computing devices (typically a server) that interface between data processing devices, such as computers, and other devices within a communications network. These devices may be located in the same local area network or in an external network (Figure 2.3) such as the Internet. A proxy server usually has access to at least two communication interfaces. One interface communicates with a device that requests services, such as a client and a device that request service (the server).

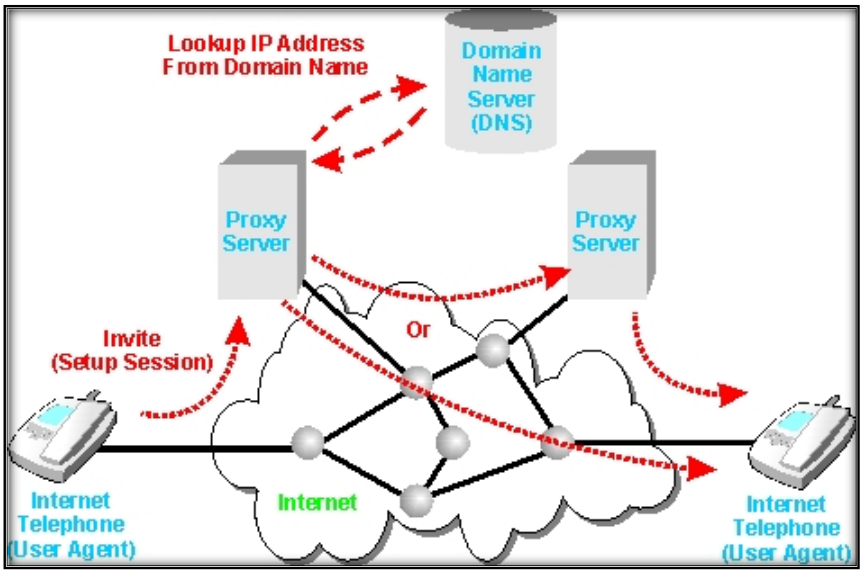

Figure 2.3: SIP proxy's relationship.

The SIP proxy is the central component of our solution (Stojsic, Radovic, & Srbljic, 2001). In Figure 2.4 illustrates an example of a standard SIP call with a proxy server that is a type of an SIP server. In the example, Alice made a call to Bob via an SIP proxy server.

However, the operations of the SIP proxy are not distinct from the HTTP or various other Internet protocols. Although this SIP proxy neither establishes nor terminates the sessions, it receives and forwards the messages by sitting in the middle of an SIP message exchange. This example demonstrates a single proxy, yet multiple proxies could exist in a signaling pathway.

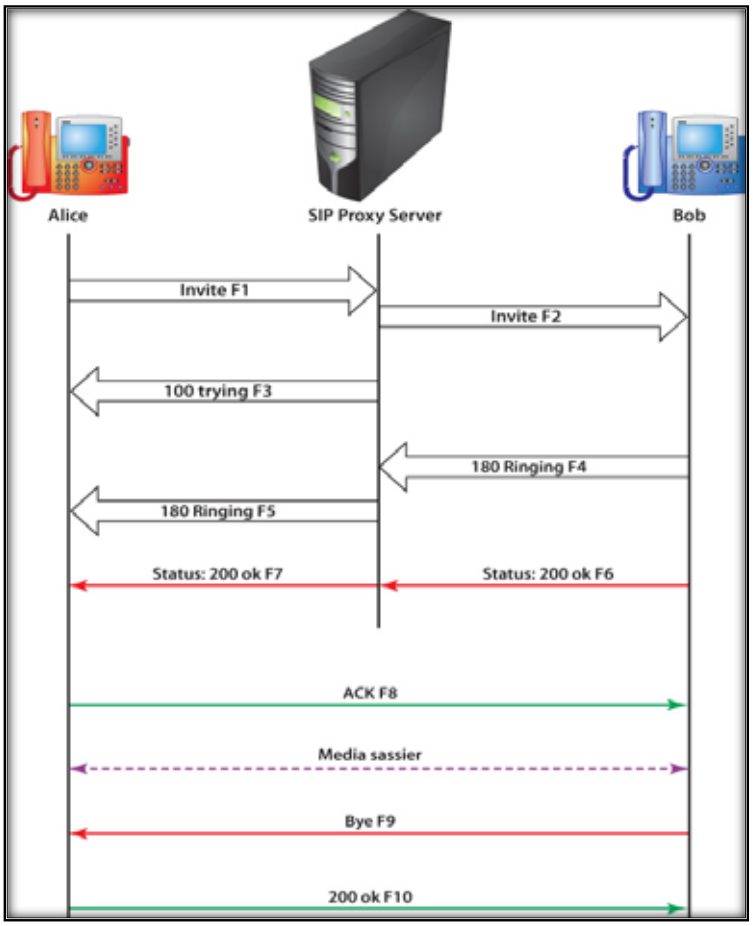

Figure 2.4: SIP call with a proxy server.

In SIP authentication requests, a request called “407 Proxy Authentication Required” requires certain responses, indicating the need for prior authentication of the phone with the proxy server, as the phone would repeat the “INVITE” request with a suitable Proxy-Authorization field if not authenticated with the proxy field (Figure 2.5).

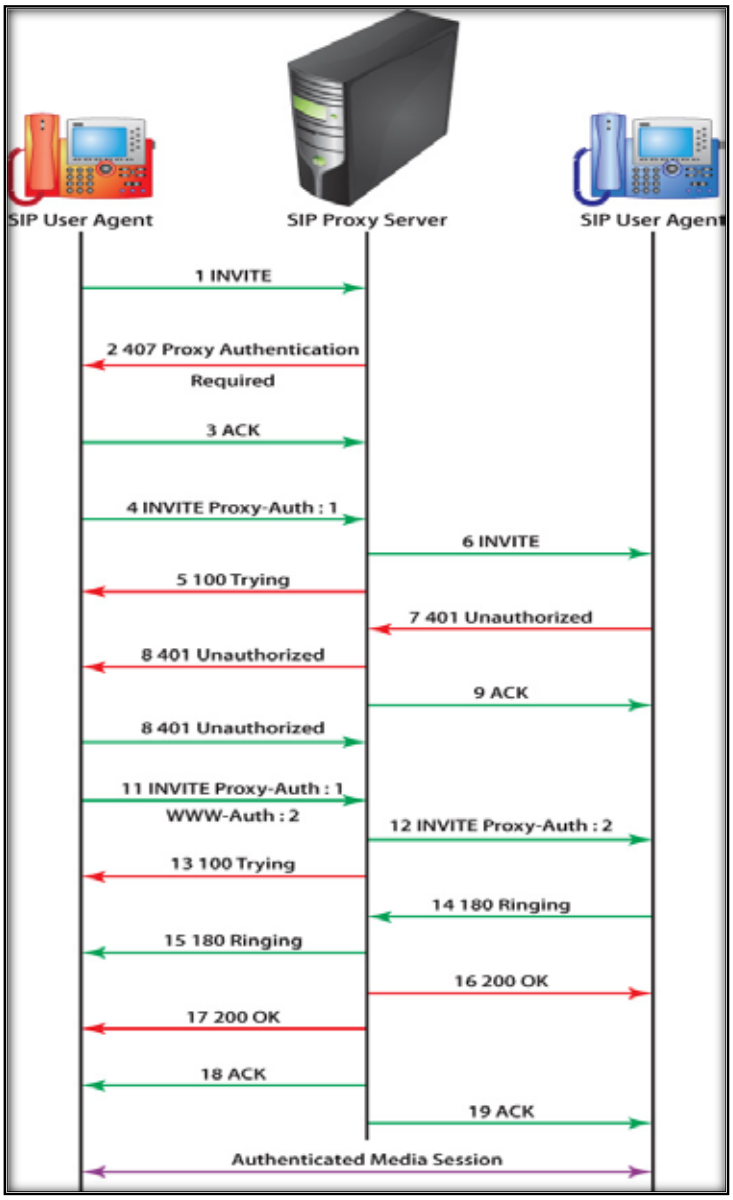

Figure 2.5: SIP transaction using authentication server.

Additionally, SIP proxy servers rewrite messages as well as forward and fork requests using the following:

- Stateful – remembers all requests (Figure 2.6).
- Stateless – forgets requests after forwarding (Figure 2.7).

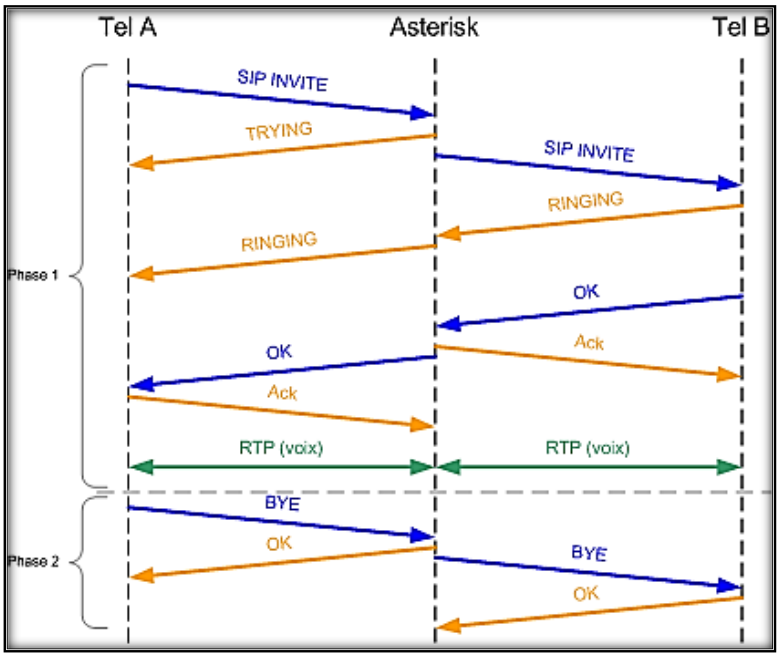

Figure 2.6: Stateful register server.

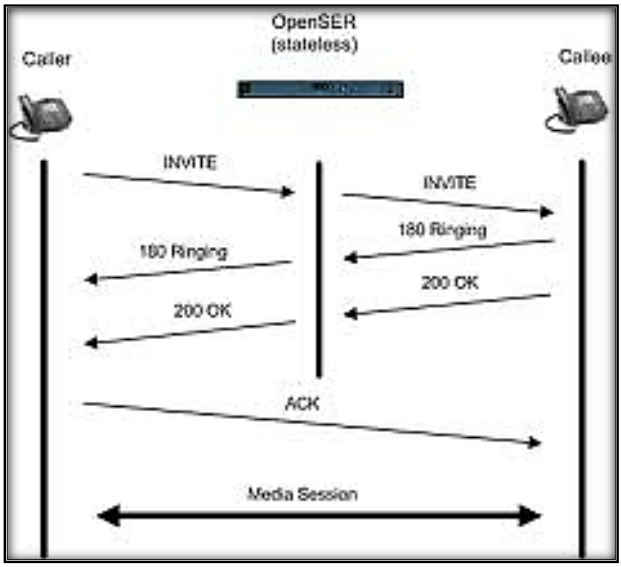

Figure 2.7: Stateless proxy server.

2.3 The RTP

The RTP (Schulzrinne, Casner, Frederick, & Jacobson, 2003) was standardized on RFC 3550. It accounts for the real-time transport of data, including audio and video, and employs the User Datagram Protocol (UDP) as the transport protocol. The audio and video data need to be packetized by a codec to allow transporting.

Basically, the protocol allows the specification of timing and content requirements of the media transmission for the incoming and outgoing packets using sequence number, timestamps, and packet forward without retransmission.

2.4 Codecs

The described contents in RTP protocol are encoded using a codec. Different codec's are designed for specified tasks; some of them possess the ability to compare and some may not.

The most popular codec is G.711 (ITU-T & Switzerland, 1988), (ITU-T & Switzerland, 1988), which does not carry out comparisons. It possesses a bandwidth of 64 Kbps for a single channel that requires a high-speed network. Such high speed is commonly found in local area networks (LANs), as purchasing a 64 Kbps bandwidth in a wide area network (WAN) can be too expensive.

2.5 A Survey on SIP

We studied taxonomy threats and clarified them to develop a framework and an overview. Moreover, we surveyed several vulnerabilities and threat mechanism issues as well as formulated some clues via high impact studies. VoIP security works are then grouped in categories described below.

2.5.1 Types of SIP Authentication

1. The following are the different types of SIP authentication:
2. Plain text authentication (no secure authentication credentials are sent over the channel)
3. Weak authentication (applied on digest authentication schemes that are common nowadays)
4. Strong authentication scheme (uses S/MIME based on personal certificates, but it is complex and costly to implement and is therefore impractical from the viewpoint of practical SIP implementation)

2.5.2 The SIP Authentication and Signaling Phase

SIP UAs register with a proxy server or a registrar. Proxy servers then act as an intermediary for SIP calls. SIP server routers that act as SIP gateways can use the services of an SIP proxy server either by contacting the server or by receiving requests from it. Additionally, UAs can register E.164 numbers with a proxy server or a registrar. An established session involves several steps, as shown in Figure 2.8.

Based on the SIP description provided previously, a hacker requires the SIP proxy, router, and gateway to obtain VoIP application privileges. Authentication is needed to verify the identity of the party with whom we are communicating. In addition, it ensures that what we receive is what they sent (integrity) and prevents unauthorized registrations. Thus, the SIP uses an authentication header and phases, as follows:

1. **Authentication phase** between user and server

2**. Invite message** from user to server /client for establishing session